Mini-AES structure

Mini-AES State

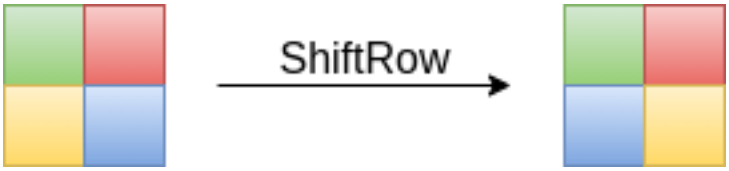
State

State size : 16 bits (4 nibbles)
Key size : 16 bits (4 nibbles)
Mini-AES irreducible polynomial: $X^4 + X + 1$

NibbleSub

Input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

ShiftRow

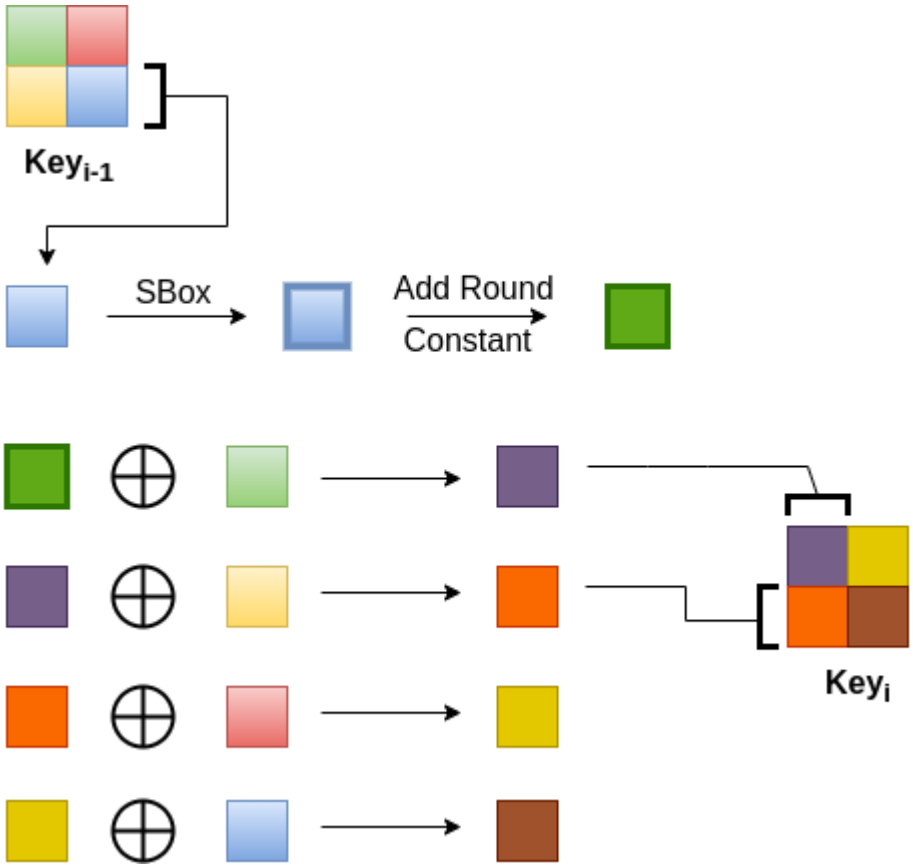


MixColomn matrix

3	**2**
2	**3**

Multiplication should be done in the field $X^4 + X + 1$

Key Schedule



Round Constants are in powers of `0x2` in the field $X^4 + X + 1$